REMARKS

This Response is submitted in response to the Final Office Action dated January 8, 2007. No new matter is added.

**35 USC §112 Rejections**

The Office Action rejects Claims 1, 5, 13, 14, 21, 22 and 23 are rejected under 35 USC §112, first paragraph, as failing to comply with the written description requirement. The Office Action states that the claims contain subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor, at the time the application was filed, had possession of the claimed invention. Applicants respectfully disagree and traverse such rejection.

Specifically, the Office Action states that the disclosure fails to recite "an additional authentication request sent from the information processing apparatus and wherein the additional authentication request is sent only if the decrypted result corresponds to the first data item, and wherein only when the user has been authenticated in response to the additional authentication request, the authentication apparatus performs processing, using the private key corresponding to the user, for making the information processing apparatus authenticate the user."

The Office Action states that the specification does not disclose, "the additional authentication request is sent only if the decrypted result corresponds to the first data item." Applicants respectfully disagree. Claim 1 reads in part, "wherein said information processing apparatus is configured to decrypt the encrypted first data item using a public key associated with the user and to compare the decrypted result with the first data item."

An example of the first data item is provided on page 9 lines 3 – 9, stating in part, "the certificate 58 includes a digital signature of a certification authority which generates the private key and the public key."

The specification, on page 10 lines 8 – 12, describes an example process where the information processing apparatus checks if the decrypted result corresponds to the first data item. The specification states, "[w]hen the WWW server 3 receives the digital signature, the WWW server 3 decrypts the digital signature by using the public key written into the user certificate received in advance. **When the decryption is successfully performed**, it is determined that the

legitimate user terminal 4 has requested the electronic priced information" (emphasis added). In this example, the digital signature was created by the authentication apparatus using the private key. See the specification on page 9 lines 20-27. A person having ordinary skill in the art would understand that the decrypted result would have to correspond to the first data item, the certificate 58 which includes a digital signature to compare against.

Additionally, the Office Action states that the specification, "does not describe an additional authentication request from the information processing apparatus." Claims 1, 13, 14, and 21-23 have been amended to traverse such rejection.

Claims 1 now reads, in part, "authenticating the data holding medium by using the common key used in the common-key encryption method for the user held by the data holding medium, ~~in response to an additional authentication request sent from the information processing apparatus,~~ wherein the additional authentication request is sent only if the decrypted result corresponds to the first data item." Claim 1 now also reads, "the authentication apparatus performs processing, using the private key corresponding to the user, ~~for making the information processing apparatus~~ to authenticate the user." Claims 13, 14, and 21-23 contain similar amendments. The amendments are fully supported by the specification.

The specification on page 10 line 13 to page 12 line 25 describes an example process where an additional authentication request is sent and, after the common-key authentication is complete, authentication is performed using the private key.

For example, the specification on page 11, lines 5-8 state, "[t]hen the CPU 46 sends the common-key-encrypted information **and an IC-card authentication request command** C4 to the encryption module 23 of the user terminal 4." The specification goes on to state, on page 11 lines 19-25, "[t]he CPU 46 of the security server 6 receives the result of authentication sent from the encryption module 23 ... [w]hen the CPU 46 confirms (in step SP45) from the result of authentication that the IC card 8 has been successfully authenticated, it obtains the private key corresponding to the user ID ... and decrypts the encrypted electronic priced information by using the private key." Therefore, an additional authentication step is performed.

**35 USC §103 Rejections**

The Office Action rejects Claims 1-23 under 35 USC §103(a) as being unpatentable over Audebert (US Patent No. 6,694,436). Applicants respectfully submit that Claims 1, 5, 13, 14, and 21-23 have been amended to traverse such rejections.

Claim 1 now reads, in part, "wherein the obtained common key encrypted transaction information is sent ~~back~~ to the data holding medium for decryption and storage." Independent Claims 5, 13, 14 and 21-23 contain similar language. The amendments are fully supported by the specification.

For example, the specification on page 12 lines 8-11 state, "[t]he CPU 27 of the IC card 8 decrypts the received common-key-encrypted electronic priced information by using a common key read from the common-key area 34 of the EEPROM 31, and writes the electronic priced information obtained by decryption into the electronic-priced-information area 33 of the EEPROM 31.

The decryption of the encrypted data and storage of said data are beneficial in allowing the data holding medium to track transactions. Additionally, the ability of the data holding medium to receive encrypted information, that can be decrypted by the medium allows for more secure communications.

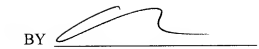
The reference Audebert does not disclose that the IC card decrypts and stores transaction data contrary to the Patent Office, relying on the reference in column 21 line 41 to column 22 line 11 as indicated in the Office Action. Additionally, it would not be obvious to a person having ordinary skill in the art to modify Audebert to include the decryption and storage of transaction data as required by the claimed invention. In Audebert, the IC card is directed towards only providing security keys and not storing transaction data.

Therefore, for at least the foregoing reasons, Applicants respectfully submit that Claims 1, 5, 13, 14 and 21-23 are patentably distinguishable and in condition for allowance.

The Commissioner is hereby authorized to charge deposit account 02-1818 for any fees which are due and owing.

Respectfully submitted,

BELL, BOYD & LLOYD LLP

BY 

Thomas C. Basso
Reg. No. 46,541
Customer No. 29175

Dated: March 7, 2007